

SIPRNet Contractor Accreditation Process (SCAP)

INDUSTRY ONLY

Contractor Accreditation Process

1. *Government Sponsor* submits validation letter to Joint Staff (J6)
2. After OSD approval, *J6* emails validation to DISA & DSS
3. *DISA* assigns DISA control number (CXXXXXX) and emails J6 letter to DSS Program Manager (PM)
4. *DSS PM* emails sponsor letter to the Sponsor & field letter to IS Rep
5. *Contractor* prepares SSP and SCQ
6. *DSS IS Rep and ISSP* works with contractor for SSP preparation
7. Contractors can now submit Master Security Plans that identify self-certification of like systems. Note: *Contractors are issued a block (based on current requirements) of IP addresses from their sponsor and they must stay within that range or request additional IP addresses from their Sponsor*
8. *DSS IS Rep* provides completed Certification Package to DAA for final accreditation and signature (No Interims) Includes SSP w/Topology (connectivity diagram) and SCQ
9. *DSS* emails/mailed signed DAA Accreditation letter and DAA signed SCQ to the contractor
10. *Contractor* emails/mailed completed Connection Package to DISA. Includes SSP, DSS DAA accreditation letter, Statement of Residual Risk with ISSM signature, Letter of Consent with ISSM signature, System Connectivity Diagram and SIPRNet Connection Questionnaire with DSS DAA signature.
11. *DISA* sends email acknowledgement of receipt to the contractor
12. *DISA* reviews Connection Package and if correct issues IATC. If not correct DISA will correspond with the contractor to resolve issues
13. *DISA* emails IATC to contractor and DSS PM
14. *DISA* runs vulnerability test (time period undetermined)
15. When system test passes, *DISA* issues ATC and emails ATC to the contractor

Open Email and Domain Name (DNS) Registration

In the past DSS provided this service for free. Starting in FY 2006 sponsors will be required to reimburse DSS when we provide these services. Budget process will start in Aug 05

1. *Contractor* must coordinate with Sponsor to see if there is a need for email/DNS
2. *Sponsor* must agree to reimburse DSS per email address and or DNS entry (billing starts in FY06, validation of accounts begin 5/05)
3. If Sponsor doesn't agree then the contractor must seek an alternative solution such as, register email/DNS with the Sponsor or stand up own email server
4. *Contractor* must fill out the registration form supplied by the DSS IS rep, which is provided in initial package
5. Contractor must submit the form to their Sponsor with the FSO signature
6. *Sponsor* must sign and email completed form to DSS PM. Incomplete forms may result in delay for services.
7. *DSS PM* will submit to DSS IT
8. *DSS* will email conformation on the black side for acknowledgement of completion and red side with user information

Disclosure Form

*Contractors are NOT allowed unfiltered access to the SIPRNet. The DoD Sponsor determine access
Joint Staff letter must have access sites identified*

1. *Sponsor* send disclosure form received from DSS PM to sites that contractors need access to
2. *Site* agrees, signs the form and submits it back to the Sponsor
3. *Sponsor* sends form to SMC smc-ctr@disa.mil
4. *DISA SMC* builds/updates contractor filter

Re-Accreditation

When authorization expires the system is no longer legal and must be terminated (looped-away). These are steps to extend the life of your system. Be advised to update packages with current information (dates, POC, system changes)

1. If *Joint Staff validation* expires then **Sponsor action required**. Follow steps 1,2 & 5-10
2. If *contract* expires then **Sponsor action required**. Submit extension letter to contractor. Contractor must submit extension letter to DSS.
3. If *accreditation* expires then **Contractor** must obtain a new Accreditation letter from DAA and submit it to DISA